ABSTRACT OF THE DISCLOSURE

COMPUTER SYSTEM AND METHOD FOR GENERATING A SELF-VERIFYING CERTIFICATE

A computer system and method are disclosed for generating a certificate that can be validated against a trusted hardware subsystem within a computer system. A security subsystem is established within the computer system. A master key pair including a master public key and master private key are established. The master private key is stored in protected storage within the security subsystem such that the master private key is inaccessible outside of the security subsystem. Generation of a self-verifying certificate is requested. A user of the computer system is then prompted to enter an authentication code in response to the request for generation of the certificate. A certificate is generated utilizing the master key pair only in response to a correct entry of the authentication code. The certificate is used only internally within the computer system.